# Access Control in Länsi-Uusimaa Department for Rescue Services: Updating the Guidelines and Procedures

Vili Harju

2020 Laurea

**Laurea University of Applied Sciences**

# Access Control in Länsi-Uusimaa Department for Rescue Services: Updating the Guidelines and Procedures

Vili Harju
Safety, Security and Risk Management
Bachelor's Thesis
May 2020

**Laurea University of Applied Sciences**
Safety, Security and
Risk Management
Bachelor's Degree

Vili Harju

**Abstract**

**Access Control in Länsi-Uusimaa Department for Rescue Services: Updating the Guidelines and Procedures**

Year 2020 Pages 32

The purpose of the thesis was to examine access control guidelines and procedures at the case organisation Länsi-Uusimaa Department for Rescue Services and update guidelines and procedures so that the security requirements would be complied at the organisation. The research questions were formed so that they would answer which are the physical security requirements that must be complied at the rescue department and how guidelines and procedures should be developed to meet the security requirements.

The thesis was conducted by using qualitative research methods document analysis and interview. In document analysis, security requirements, standards and best practices concerning access control were reviewed. Interviews were done with security management professionals from other organisations and their knowledge of the topic complemented the results from document analysis.

The outcome of the thesis process was two products, access control policy and incident response manual, which would help the case organisation to achieve the desired level of security and meet security requirements. The access control policy underlines the responsibilities and principles for secure use of the facilities. Incident response manual helps organisation to resolve possible incidents in efficient manner.

The final products can help the organisation to meet the security requirements if guidelines and practises are applied in the case organisation. This will require training and communication inside the organisation and change in familiar working practises. The introduction of the products is left out of the thesis scope.

Keywords: access control, physical security, rescue department

**Laurea-ammattikorkeakoulu**
Safety, Security and
Risk Management

Vili Harju

**Tiivistelmä**

**Kulunvalvontaohjeiden ja -käytäntöjen päivittäminen Länsi-Uudenmaan pelastuslaitokselle**

Vuosi 2020 Sivumäärä 32

Tämän opinnäytetyön tarkoituksena oli tutkia ja uudistaa Länsi-Uudenmaan pelastuslaitoksen kulunvalvonnan ohjeita ja käytäntöjä. Opinnäytetyön päätarkoituksena oli luoda päivitetyt ohjeet niin, että ne vastaavat pelastuslaitoksia koskeviin turvallisuusvaatimuksiin. Tutkimuskysymykset muodostettiin niin, että ne auttaisivat selvittämään mitkä turvallisuusvaatimukset koskevat pelastuslaitoksia sekä miten ohjeita ja käytäntöjä tulisi kehittää turvallisuusvaatimusten täyttämiseksi.

Opinnäytetyön tiedonkeruunmenetelminä käytettiin laadullisia tutkimusmenetelmiä dokumenttianalyysiä ja haastattelua. Dokumenttianalyysissä tarkasteltiin kulunvalvontaa koskevia turvallisuusvaatimuksia, standardeja ja hyväksi havaittuja käytäntöjä. Haastatteluissa kuultiin turvallisuusasiantuntijoita ulkopuolisista organisaatioista ja asiantuntijoiden tietämys aiheesta täydensi dokumenttianalyysin tuloksia.

Opinnäytetyön tuloksena syntyi kaksi tuotetta: kulunvalvonta ja -hallintapolitiikka sekä ohje kulunvalvontatapahtumien selvittämiseen. Tuotetut dokumentit auttavat pelastuslaitosta täyttämään turvallisuusvaatimukset sekä korottamaan turvallisuustasoaan. Kulunvalvontapolitiikassa esitetään yhteiset käytännöt sekä vastuut tilojen turvalliselle käytölle koko organisaatiossa. Ohje kulunvalvontatapahtumien selvittämiseen edesauttaa tilanteiden nopeaa ratkaisua.

Opinnäytetyön tuotteet auttavat Länsi-Uudenmaan pelastuslaitosta täyttämään turvallisuusvaatimukset, kun organisaatio ottaa päivitetyt ohjeet käyttöön. Tämä edellyttää työntekijöiden kouluttamista sekä viestintää organisaation sisällä, jotta työtapoja voidaan muuttaa. Ohjeiden käyttöönotto on jätetty opinnäytetyön ulkopuolelle.

Avainsanat: kulunvalvonta, fyysinen turvallisuus, pelastuslaitos

Table of Contents

# 1 Introduction

The purpose of the thesis was to examine and renew access control guidelines and procedures at the case organisation Länsi-Uusimaa Department for Rescue Services. The primary purpose of the thesis was to create updated guidelines and procedures based on the security requirements which must be complied at the case organisation. The best practices of the security controls were also discovered in the research process and applied in the creation of the final products. In addition to access control and management, the thesis deals with the visitor management and key control. The goal was to create and update guidelines and procedures so that they can be deployed across the organisation as easily as possible with existing technical solutions and focusing on administrative processes and employee behaviour. Risk assessment approach as part of the development of the guidelines and procedures is left out of the thesis scope.

The form of the thesis was functional study as the thesis aimed to provide updated guidelines for case organisation. This thesis was based on the needs of the organisation and agreed together with the Head of Support of the rescue department. The topic was chosen as existing guidelines and procedures required revision and the working environment was changing as rescue departments in Finland are adapting to use the Government Security Network more broadly in the future.

The purpose of the Government Security Network is to provide under normal and disruptive conditions and in exceptional circumstances, uninterrupted and continuous communication required by the cooperation of the government, public safety authorities and other actors. The rescue departments are obligated to use the Government Security Network. (Finland 2015.) The principles of operation and use of the network include high precautions and information security requirements (Valtiovarainministeriö 2015).

Updated access control guidelines and procedures for the Länsi-Uusimaa Department for Rescue Services will help the organisation to meet the security requirements and to improve organisation's overall security capability and awareness.

The research questions were formed in the beginning of the thesis process as following:

1) Which security requirements should be taken into account when developing rescue department’s physical security?

2) How should the guidelines and procedures be designed to meet the security requirements?

The thesis process produced updated access control policy for the case organisation, access control guidelines and response procedures for situation center operators who monitor the access control system and induction material for new employees to promote security awareness concerning physical security.

The thesis report presents how guidelines concerning access control and its management can be developed based on the research results, but the final products developed for the case organisation are left outside the thesis report due confidentiality reasons.

## 1.1 Case organisation

In Finland, rescue services are carried out by regional rescue services. The responsibilities of rescue services are jointly managed by municipalities of a certain region designated by the Government. Regional rescue services must have a rescue department. Duties of rescue departments are mandated in the Section 27 of the Rescue Act and include the responsibilities to carry out rescue operations, to provide guidance and education in preventing fire and other accidents in their region among other duties. The standard of service of the rescue services must meet the local requirements as well as threats of accidents. Obligation of effective performance of duties lies on rescue department as rescue operations must be carried out without delay and in appropriate way. (Finland 2011.)

Länsi-Uusimaa Department for Rescue Services is one of Finland's 22 rescue service providers and forms part of the City of Espoo's organisation (Ministry of the Interior 2019; Länsi-Uusimaa Department for Rescue Services 2017). Twelve full time rescue stations, in ten municipalities within the region, are in charge of performing fire and rescue operations around the clock. In addition to full time stations, there are 40 volunteer fire stations operating in the region. Länsi-Uusimaa Department for Rescue Services employs 600 persons and approximately 1000 voluntary fire fighters are working for contract fire brigades. (Länsi-Uusimaa Department for Rescue Services 2017.)

The 600 employees of the rescue department work in various tasks: duty officers, firefighters and emergency medical personnel are on constant standby and seen on the field, but rescue department employs fire preventing officers, risk management professionals, communication, IT and technical professionals as well as human resources and administrative staff to support daily rescue operations.

## 1.2 Working environment

The rescue departments are obligated to perform their duties without delay. Various threats might endanger facility security of the rescue department and therefore cause harm to protected assets such as personnel, vehicles, critical information technology and communication

equipment, information and facilities. The continuity of the rescue operations might be endangered even if a single asset is compromised.

12 full time fire stations are located around the Western Uusimaa region and the central fire station is located in Espoo. Central fire station facilities are in daily use of the operational rescue staff as well as administrative and office staff, situation centre and workshop personnel work in the premises. Other fire stations located in Espoo and in other municipalities mainly consist of small office spaces for fire prevention officers in addition to lounge spaces for operational rescue crew, vehicles and maintenance equipment. (Länsi-Uusimaa Department for Rescue Services 2017.)

Some of the contract fire brigades are located in the same facilities as rescue department but otherwise contract fire brigades operate from their own facilities. Therefore, they are left out of this thesis and thesis products will not address how the access control practises should be managed among contract fire brigades.

As fire stations are located in various municipalities, the owners of the facilities vary as well. In cooperation with the owners, the common understanding of responsibilities and rights concerning physical security must be agreed.

# 2 Theoretical framework

In this section, context to the topic is expressed in the form of the theoretical framework based on relevant literature and other documents. Theoretical framework is a system of concepts where concepts and their relation to the topic are defined (Ojasalo et al. 2014, 25). In this thesis, the theoretical framework consists of approaches to physical security and security requirements.

## 2.1 Physical security

Physical security is used to protect facilities, people, information and other assets by physical controls. The physical security measures ensure that only the persons with authorization are able to access facilities and assets. Measures within the facilities must be employed appropriate for operating environment and levels of asset protection. (Fennelly 2013, 339.)

Physical security controls deployed will depend on protected assets and facilities: where these assets are located and “what are the threats, vulnerabilities and risks” threatening these assets. The utilization of physical security controls should be addressed in layers. (Kovacich & Halibozek 2003, 186.) Layered approach will help security controls complement each other’s in overall asset protection. In layers, various physical security controls such as physical barriers, locks, access controls, alarm systems and camera surveillance accomplish facility’s physical protection against various threats (Fennelly 2013, 82).

### 2.1.1 Access control

The aim of access control, according to Kovacich and Halibozek (2003, 200), is to ensure proper authorization of persons entering the premises so that risks against assets are reduced. In addition to other physical security controls, Fennelly (2013, 257) expands on the goal of access control system and procedures as help to prevent persons without authorization to enter the facilities. Access control systems include various devices such as “locks, ID cards, entry devices and door alarms” to guarantee that the personnel and authorized visitors are able to gain entry (Lorenzi 2018, 46-49). Electronic access control systems employ computer software, as well as various devices such as credential reader and door locks connected to the system control panel. The system enables that each authorized user can be validated for given areas within the facilities as well as combine an alarm monitoring element that notices when alarmed doors are force opened. (Norman 2012, 28-31.) Credential readers read given credentials and verifies identity data against the database which includes information of authorized users (Norman 2012, 31).

The monitoring of the access control events is an important part of the protection. When doors are locked and alarmed, the system operates as an intrusion detection system and allows security guard or some other entity to monitor events from the software and start the response procedures if needed. In the access control system, other devices such as surveillance cameras can be integrated to the system and used to verify intrusions as cameras can be connected to certain alarmed areas. The access control system records the access events and allows log revision afterwards. (Norman 2012, 28-31.)

### 2.1.2 Visitor management

Well controlled visitor management system improves the physical security management in the organisation. Precautions against criminal activity require the “screening, identification and control of visitors”. Visitors are first identified and registered as they arrive to facilities, and they gain visitor card or badge at the beginning of the visit. (Terschuren 2016.) Visitors should be required to hand badges back when the visit ends. Precautions such as expiration date on visitor badge can be placed to prevent unauthorized reuse. Visitors should stay along with their assigned hosts and hosts are responsible for their companion. (Fennelly 2013, 261.) Visitor badge may include information of escort and specific areas where visit is allowed. Badge should also clearly indicate the difference to employee identification so recognition and controlling visitors is easier (Kovacich & Halibozek 2003, 203.)

### 2.1.3 Key control and management

Locks are important part of physical security protection, but insufficient key control can turn locking devices useless. Keys and locks should be accounted, and keys should be distributed to employees on a basis of where they need to execute their work. Record of personnel handling specific keys should be updated and information of lost or stolen keys should be reported so actions can be made. Annual review of keys and locks should be made to see if there are any losses or changes on quantities. (Kovacich & Halibozek 2003, 198.)

## 2.2 Security requirements

According to Cambridge Dictionary (2020a) requirement is something you are obligated to do. The Open Security Architecture (n.d.) describes security requirement as a level of security objectives, which are raised by "regulations and laws, best practices and standards and perceived end user needs". Some of the security requirements presented in the following sections are obligatory for rescue departments and some act as a standard or guideline for implementing security controls to achieve desired security objectives.

### 2.2.1 Legislation

The Act of Openness of Government Activities sets the ground to obligation of the public authorities to prevent material abuse. In order to establish and implement good information management practices, the authorities shall ensure that the documents and information systems are secured. (Finland 1999.)

The Government Decree on Information Security in Central Government 681/2010 provides general information security requirements to document handling by central government authorities. The Decree is meant for central government authorities defined in the Degree such as state administrative authorities and government agencies. (Finland 2010.) In the information security manual for rescue departments by Pelastuslaitosten kumppanuusverkosto, unofficially translated to the Cooperation Network of Rescue Departments in Finland (2019), it has been defined that the guidelines for rescue departments are drawn based on the Decree and therefore rescue departments should fill the basic level of information security implementation defined in the Government Decree 681/2010. The basic level requirements include risk assessment connected to activities, proper documentation, variety of information security controls such as security arrangements on networks and systems and sufficient monitoring and protecting premises where data is processed, and documents are stored. Section 14 of the Decree lists physical security requirements for premises as classified documents should be "protected by means of appropriate locks, access control and other measures to prevent unauthorized access to the premises". (Finland 2010.)

The new Act of Information Management in Public Administration, translated from Laki julkisen hallinnon tiedonhallinnasta, came into force in the beginning of 2020 and its application is required from other entities e.g. municipalities and universities as well than just central governmental authorities. Security requirements presented in the Act share similarities from information security perspective with the Government Decree 681/2010. The Act requires e.g. identification of facilities and systems where information is handled (Finland 2019; Deloitte 2019.)

Access control system collects personal data as movements of credential holders are readable from the system and stored as well as real-time monitoring of employees' movements can be done through the system. Therefore, GDPR, the General Data Protection Regulation of the European Union should be taken into account when deploying access control system: what identifiable information is collected, who is able to process information, where information is stored and how long. (EU 2016.)

### 2.2.2 KATAKRI and VAHTI

Katakri is a Finnish acronym for the information security audit tool for authorities. Katakri aims to assess companies' and organisations' capabilities to handle classified information and to assess companies' readiness to Facility Security Clearance carried out by authorities. The first version of Katakri was published in 2009 and the current version available is from 2015. (Ministry of Defence 2015.)

Katakri combines together security requirements based on Finnish legislation and international information security obligations from the European Union level. An important reference material and baseline for security requirements in Katakri is aforementioned Decree on Information Security in Central Government 681/2010. Still, the security requirements in Katakri are not definite. (Ministry of Defence 2015.)

Katakri consist three subdivisions: security management, physical security and information assurance. Subdivision physical security approaches protecting information from unauthorised disclosure. Requirements for access control are given in detail as topics include: "deterring unauthorized access" and "management of access rights". (Ministry of Defence 2015.)

VAHTI, the Finnish Government Information Security Management Board provides comprehensive information security instructions administrated by the Ministry of Finance. VAHTI-instructions cover all the areas of information security from different point of view, including physical security. (Ministry of Finance n.d.) VAHTI-instructions are widely used and applied in central government and public administration. VAHTI 2/2013 Office premises information security instructions provides detailed guidelines to plan and implement security controls in facilities to protect information from unauthorized disclosure (Valtiovarainministeriö 2013).

# 3 Methodology

The thesis was conducted as functional study of how access control guidelines should be implemented in the case organisation so that the guidelines meet the security requirements. The research approach in this thesis process was constructive research as Ojasalo, Moilainen & Ritalahti (2014, 37) describes it appropriate for research where practical problem must be solved and new construction such as "product, information system, guideline or manual, method or plan" is developed. To develop new construction such as guidelines, existing theoretical knowledge and collected new empirical knowledge is required. Constructive research aims to gain information on practical problem which is theoretically justified and brings new knowledge to the community. (Ojasalo et al. 2014, 65.) Implementation of the developed solution and evaluation of its practical functionality is an important part of the constructive research process and will be taken into consideration in the assessment phase of the thesis (Ojasalo et al. 2014, 38). According to Ojasalo et al (2014, 65) using constructive approach requires communication from the researcher and the party who has issued the project. Assessment of developed product emphasises the communication between parties. Ojasalo et al. (2014, 67) suggests that in the end of the process, multiple versions of solutions should be presented and assessed, and the chosen final solution must be justified.

## 3.1 Research methods

Typically, research methods in constructive research vary and as the research aims to develop new solutions for case organisation, multiple methods should be applied (Ojasalo et al. 2014, 68). Constructive research methods can be both qualitative and quantitative (Oyegoke 2011, 579). According to Saunders (2015, 725) qualitative data is non-numerical data which is not quantified but quantitative data is both numerical and quantified. Qualitative research methods aim to "detailed description of processes and views" (Flick 2011, 252). This thesis was conducted by using qualitative research methods: document analysis and interviews.

### 3.1.1 Document analysis

The document analysis method is suitable research method for situations where conclusions are made from the written documents. Originally, the written documents may have been other materials such as conversations turned later into transcripts or even pictures. (Ojasalo et al. 2014, 136.) Critical thinking should be applied while conducting document analysis on who has produced the document and for what purpose (Ojasalo et al. 2014, 43). The process of document analysis is described by Ojasalo et al. (2014, 138) in Figure 1.

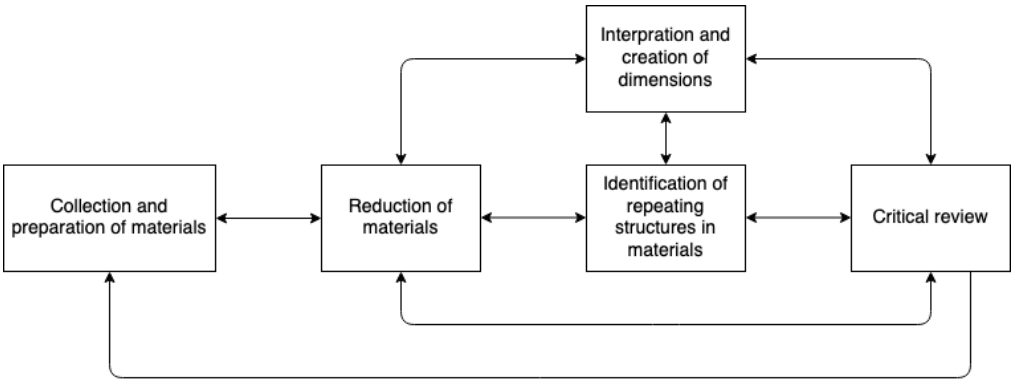


Figure 1: Document analysis process (Ojasalo et al. 2014, 138)

The purpose of the document analysis in this research process was to define substantial information from reference materials which would be relevant for access control guidelines' and procedures' development. Reference materials include materials expressed in theoretical framework, existing guidelines from case organisation and verbal material collected from interviews, turned in to written form by processing data.

### 3.1.2 Interviews

According to Ojasalo et al. (2014, 65) new constructions such as guidelines require existing theoretical knowledge and new empirical knowledge. Interview was chosen to thesis as a research method to collect new empirical knowledge, because interviews aim to clarify and deepen the knowledge of certain topic and through interviews data collection from individuals is rather easy (Ojasalo et al. 2014, 106). According to Hirsjärvi & Hurme (2000, 14) interview as qualitative data collection method is flexible and suits for various purposes. The disadvantages of using interview described by Hirsjärvi & Hurme (2000, 35) are that interviewer's maturity to interview may distract the objective of interview, interviews take time as suitable interviewees must be found and conducting and analysing the interview is time-consuming. The reliability of interview and results is challenging and should be taken into account so that results will not endanger the purpose of research (Hirsjärvi & Hurme 2000, 35).

The purpose of the interviews was to obtain best practices as well as new perspectives from physical security professionals on how to develop and implement access control guidelines and procedures. Interviews were done by using semi-structured interviews where interviewer has "list of themes and possibly some key questions" ready, but "their use may vary from interview to interview" (Saunders 2015, 391). For semi-structured interview is typical that the themes are decided beforehand, but they are not definite (Hirsjärvi & Hurme 2000, 47). According to Saunders (2015, 394) the advantage of using semi-structured approach is good in a situation where questions may be "complex or open ended" and "logic of questioning may need to be varied". Semi-structured interview also allows that some of the pre-planned

questions can be left unasked and some additional questions can be asked during the interview (Ojasalo et al. 2014, 108).

Interviewees i.e. research participants were selected and contacted based on their role in the organisations from similar operational environments and what is their relation to the topic. Permission to interview was sent to research participants beforehand and they were given a chance to choose whether they allow interviewer to voice record the conversation or not. Research participants are presented in the table in Results section 4.2. As suggested by Ojasalo et al. (2014, 107) interviews were recorded to ease interviewer's attention from making notes.

# 4 Results

The collected data was analysed by using a qualitative analysis model Ojasalo et al. (2014, 138) presented. After materials were collected and prepared, including the analyses from interviews, irrelevant material was redacted. After redaction, the interpretation from material was made to identify the repeating themes. In the critical review, conclusions were drawn by using techniques such as "pattern finding, noting relations between variables and building a logical chain of events". (Ojasalo et al 2014, 143-144.)

The results from the data collection are presented in sections divided by their collection methods. The results were analysed by using the same methodology and summarised results are presented at the end of the chapter.

## 4.1 Document analysis

The materials for document analysis were chosen as suggested by Ojasalo et al. (2014, 43) by assessing who has produced the document and for what purpose. The analysed materials were mostly meant for governmental agencies and rescue departments, but also more generic guidelines and standards were analysed to provide a more comprehensive understanding of the physical security requirements in various operating environments. The analysed materials and their justification are presented in the Appendix 1.

The most important materials from the security requirement perspective are presented in Figure 2 as well as their relations. According to Ojasalo et al. (2014, 143-144) in the critical review of materials, the discovery of relations between variables in the materials is an important part of the analysis process. The graph also presents an answer for research question "Which security requirements should be taken into account when developing rescue department's physical security?" as definite security requirements are coming from legislation that must be complied in the organisation. By developing guidelines and procedures based on security requirements, the basic level of compliance is achieved when guidelines and procedures are applied in the organisation.

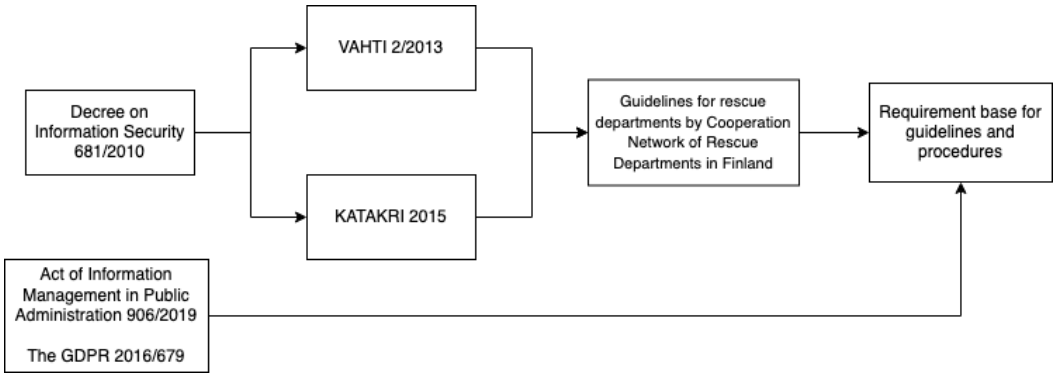


Figure 2: Security requirement base for guidelines and procedures

Figure 2 presents that the access control guidelines for the case organisation Länsi-Uusimaa Department for Rescue Services should be developed by taking into account the guidelines for rescue departments by Cooperation Network of Rescue Departments in Finland, which are based on KATAKRI and VAHTI-instructions. The base for KATAKRI and VAHTI 2/2013 Office Premises Information Security Instructions is again coming from the Decree on Information Security 681/2010 so rescue departments would fill the basic requirement of information security stated in the Decree by implementing security controls and procedures defined in these guidelines. Another important and affecting legislative regulation for rescue departments is the Act on Information Management 906/2019. According to this Act (Finland 2019) the information must be processed and stored in facilities where confidentiality, integrity and availability of the information must be guaranteed by security controls. In theoretical framework, the similarities between the Decree on Information Security 681/2010 and Act on Information Management 906/2019 are presented and therefore by following the basic information security requirements mandated in Decree 681/2010 concerning physical security controls, the information security requirement on the Act 906/2019 is fulfilled.

Security requirements from the GDPR (2016) outlines that organisations should implement “appropriate technical and organisational measures” to ensure secure processing of the personal data. This is another regulatory requirement which must be complied at the case organisation.

Other materials used in the document analysis weren’t obligatory security requirements for rescue departments but suggestions or standards how to implement security controls so that a certain level of desired protection would be achieved. Supporting materials for broaden understanding of physical security and access control were:

- SFS-EN 60839-11-2 Electronic access control system. Application guidelines by Finnish Standards Association SFS

- Avainturvallisuusohje, secure key control guidelines by Finance Finland

- ISO/IEC 27002:2017 Information technology. Security techniques. Code of practice for information security controls by Finnish Standards Association SFS

- And Facility Security Requirements by TAPA: Transportation Asset Protection Association, later called by TAPA FSR

Organisation's current access control guidelines were also reviewed in the analysis process, but the results of reflection between current guidelines and requirements are not published as part of the thesis report due confidentiality reasons as well as security guidelines by the Cooperation Network of the Rescue Departments in Finland are left out of the published analysis. In the analysis of the material, pattern finding as well as learning logical chain of events were used as suggested by Ojasalo et al. (Ojasalo et al 2014, 143-144). In following sections, results are presented in patterns.

### 4.1.1 Access control management and monitoring

Important part of the access control management is to grant access rights for personnel based on classification of the facilities and personnel's need to perform their duties in facilities as well as on the least information principle. Organisation should have designated person granting and maintaining the access rights, and document of the access rights should also be reviewed regularly and updated if personnel of the organisation changes positions. (KATAKRI 2015, VAHTI 2/2013, TAPA FSR.) The areas where more sensitive information is processed and stored in the facilities is controlled more strictly with controls such as two-factor authentication (KATAKRI 2015; ISO/IEC 27002:2017).

Organisation should document the access control procedures as well as instruct personnel on procedures such as provide and request personnel to use ID cards and comply with instructed visitor management procedures. Organisation has the responsibility to instruct personnel to react on security events such as unauthorized persons in the facilities. Reaction itself is not enough so procedures on what to do next and where to contact in a case of security event should be documented and instructed. Working in the facilities and in certain secure classified areas must be instructed for personnel to ensure security in the use of the facilities, so that any assets will not be compromised. (KATAKRI 2015, VAHTI 2/2013, TAPA FSR.)

All personnel in the organisation should be able to react on visitors without visitor badges or escorts and inform the security staff of the situation (ISO/IEC 27002:2017). Access control events can be monitored from the electronic access control system and the system users and operators should have enough training to use such system efficiently. The system owner must provide enough guidance for users and operators as well as motivate them to security culture. (SFS-EN 60839-11-2.) Important requirement for the system operators is that they will react on security events without delay 24/7/365. The response procedures should be documented.

(SFS-EN 60839-11-2, TAPA FSR.) The access events or access logs should be stored for a certain timeframe and reviewed, especially on facilities with the higher security classification (KATAKRI 2015; ISO/IEC 27002:2017).

### 4.1.2 Visitor management and key control

Organisation should have documented and instructed visitor management procedures. The information of the visitation should be collected beforehand and include at least the following aspects: the date and time of the visit, visitors' names and organisational information, host and facilities used during the visit. At the time of the visit, visitors are identified with proper identification method, registered and the visitor badges are given. The host from the organisation should stay alongside the visitors during the visit and inform visitors of security requirements and emergency procedures in the facility at the beginning of the visit. The registration may include signing non-disclosure agreement. (KATAKRI 2015, VAHTI 2/2013, TAPA FSR, ISO/IEC 27002:2017.)

The maintenance and cleaning personnel should be treated with the same basis as visitors. Their access rights should be limited and based on facilities classification, their presence in certain areas of the facilities should be monitored and registered. (KATAKRI 2015; VAHTI 2/2013.)

Organisation should have designated person in charge of the key management including storing the keys and key distribution. Keys are granted for individual persons based on their need to access certain areas of the facilities. (Avainturvallisuusohje; TAPA FSR.) Organisation should also document the reason why keys are submitted (KATAKRI 2015). The user of the key should sign the document to proof the transaction and receiver should be informed about responsibilities related to handling key securely. The user of the key is obligated to inform the organisation if he or she loses the key. (Avainturvallisuusohje, TAPA FSR.) Guidelines and requirements concerning keys are applied in this thesis to handling access credentials.

After careful analysis of documents, I was able to understand more thoroughly what the definite requirements for rescue departments are as well as what physical security control suggestions would help the rescue departments to meet the security requirements and raise their overall security capacity. Based on the document analysis, I was also able to identify what kind of information should be collected through interviews to understand more thoroughly how guidelines and procedures should be designed.

## 4.2 Interviews

The interviewees i.e. research participants were selected as described in the Methodology section. The invitation to interview was sent to seven persons in the January 2020 and three of them agreed to participate. The interviews were done in January and February 2020 in

Helsinki metropolitan area. The length of the interviews varied from 45 to 60 minutes. The table below presents the research participants and their expertise in physical security as well as their experience in a certain working environment

| | Position | Experience | Relation to physical security | Working environment |
|---|---|---|---|---|
| Interviewee 1 | Security Manager | Over 10 years | Overall security management of the organisation including physical security and the development of the situational awareness | Rescue services |
| Interviewee 2 | Senior Specialist | Over 10 years | Specification of physical security requirements for service providers, guidance, preparation and development of the internal regulations | Government |
| Interviewee 3 | Security Manager | Over 15 years | Lead security management and preparedness in the organisation | Municipal |

Table 1: Research participants

Overall, data collected through the interviews answered the second research question "How the guidelines and procedures should be designed to meet the security requirements?" The interview questions were drawn based on document analysis process' results and topics were decided so that expected results from interviews would help in developing the guidelines and procedures. The interview questions were planned to ask in the themes and questions are visible in the Appendix 2. The semi-structured interview allowed interviewer to ask additional questions during the interview and modify order of the questions as Ojasalo et al. (2014, 108) and Saunders (2015, 391) presented.

In this section, the analysed results from the interviews are presented in themes as following:

### 4.2.1 Responsibilities among personnel

As document analysis concluded, the access control and its management require various responsibilities from both personnel of the organisation as well as from security or facility management professionals in the organisation. In the interviews, I was interested to hear professionals' opinions about responsibilities. All interviewed professionals agreed that it's not that relevant to decide in the organisation whether the security or facility unit manager or professional is in charge of the access control management as long as there's enough subject knowledge and other resources available to plan and implement processes. (Interviewee 1; Interviewee 2; Interviewee 3.) If responsibilities in the organisation lie within facility

manager or other non-security professional, there should be consultation available from security professional to support decision making and planning concerning access control management or system from security point of view – vice versa, if security professional needs support in facility management related issues. (Interviewee 2.)

Responsibilities of the employees cannot be emphasised as they are the users of the facilities as well as users of the access control systems. Employees are 'the eyes in the facilities' and able to detect unauthorized persons or other events which require immediate actions. Employees anyway cannot react unless they have taught to identify such events and they are informed of the action procedures. Employees are the main users of the facilities and it is organisation's responsibility to inform them about company or organisation level policies of visitor procedures or usage of access control system. (Interviewee 1, Interviewee 2, Interviewee 3.) If employees are well educated on organisational security procedures, they will feel like security culture in the organisation is taken seriously and employer is interested to support personnel security in the organisation (Interviewee 2).

Responsibilities of the managers or supervisors were discussed and how they should be the key communicators in the facility security related issues in addition to security professionals. Usually, manager or team supervisor is responsible for induction of the new employee so managers and supervisors should have enough knowledge and materials available to train new employees to accepted procedures. If organisation develops its procedures concerning e.g. visitor management procedures, these changes should be communicated from the top of the organisational chart so that the message would be distributed to whole organisation as well as its reliability and importance would be taken into account. (Interviewee 1.) Professionals also agreed that communication and reminders of general procedures related to facility security should be shared in the organisation periodically so that all themes of the organisational security are familiar to all personnel. (Interviewee 1; Interviewee 2; Interviewee 3.)

The importance of the documentation as part of the responsibilities was pointed out by one of the interviewed professionals as responsibilities overall may accumulate on one person in the organisation and the continuity of the operations and knowledge may be endangered if professional is unable to perform his or her duties. This kind of situation would be e.g. if person in charge of granting access rights is unable to perform the job, someone should have enough knowledge to continue the work so that the access rights are given on a same basis and based on documented procedures. (Interviewee 1.)

### 4.2.2 Identification and monitoring of security incidents

Heavily depending on facilities and operational working environment, the monitoring of access control system and events differs from security guards to the main user of the system. Professionals summarised that electronic access control system and other technological

solutions such as camera surveillance are supporting tools in access control and the monitoring and the identification of the events happens among the personnel who are instructed to do so. (Interviewee 1; Interviewee 2; Interviewee 3.)

Identification of security incidents or potential incidents should be instructed to all personnel. The instructions should include case-examples so that employees would understand the different kind of intrusion methods or what might happen if doors are kept open in facilities against the guidelines. (Interviewee 3.) Employees should be trained to understand that security culture and awareness is part of daily business and operations. (Interviewee 1; Interviewee 2; Interviewee 3.)

One of the professionals described that the process after an employee has made and reported an identification of security incident in overall is important as it indicates organisation's maturity to react and solve security incidents. If incident is reported to designated person or unit, there should be obviously immediate actions to solve and fix the incident, but the employee who has identified and reported the incident should be informed of taken actions and 'praised' for his or her actions. (Interviewee 2.) The communication may increase organisation's security awareness and culture and encourage other employees to take actions as well in the future (Interviewee 2; Interviewee 3).

### 4.2.3 Maintenance and other contractors in the facilities

The third theme discussed with the professionals concerned maintenance and other external contractors who needs to access facilities daily or occasionally when needed. This topic is tied to the visitor management as the processes follow the same principles. All professionals described that organisation should have different processes for known maintenance or cleaning personnel who accesses the organisation daily basis and for maintenance or other operators who visits the facilities when needed. The known permanent maintenance or cleaning personnel might be obligated to provide security clearance to access facilities, and they have their own access credentials which allow them to access pre-classified areas of the facilities individually. To access areas with higher security classification might require the presence of other employees from the organisation. (Interviewee 1, Interviewee 2, Interviewee 3.) Process for other maintenance visitors such as contractors is described in the next section.

One of the professionals suggested that various visitor groups including contractors would be pre-classified and their access rights would be decided and limited beforehand if they have need for access credential to ease movements in the facilities during the work. Still, if access credentials are made and given for contractors, credentials should be registered for individual users and their responsibility to secure handling would be the same as for any personnel. The access credentials should be collected from contractors by the end of the day and returned next morning when work continues at the facilities. (Interviewee 1.)

The non-disclosure agreement is an important document for every visitor but especially for visitors such as maintenance contractors and cleaning personnel as their access rights in the facilities might be more extensive. Professionals suggested that if organisation or company uses regularly same contractors e.g. on telecommunication, they would acquire list of maintenance personnel from contractor companies so that authentication of contractors at the facilities would be easier and more secure. (Interviewee 1, Interviewee 2, Interviewee 3.)

### 4.2.4 Visitor management

All interviewed professionals emphasized the importance of the well-controlled visitor management processes and how visitor management is not only about how visitors are treated in a good and respected manner at the organisation but how visitations shouldn't endanger any organisation's assets. Employees of the organisation or company should always be aware of visitor policy, so fundamentally that requires organisations to develop policy if they don't have one already. (Interviewee 1; Interviewee 2; Interviewee 3.)

Professionals generally described the visitor management procedures in a same manner as described in the 4.1 Document analysis section but added some details how employees can be motivated to comply with the policies. Professionals suggested that while employees are 'forced' to comply with the strict company-level guidelines, the benefits for doing so should be described as well. Employees should understand that the procedures are made to smooth both visitation and employee's daily life if visitation can go effortlessly without any extra paperwork or misunderstanding. (Interviewee 1; Interviewee 2.) Visitors are guests and they are able to see how procedures are managed in the company or organisation and this can be seen as a public relation matter as public image in certain operating environments should be e.g. security driven (Interviewee 2).

### 4.2.5 Developing the procedures

Finally, I asked professionals' opinions and experiences how they have approached the development of the procedures and what would be the indicators for the need of the development. Professionals described that the development can be based on system monitoring e.g. where electronic access control system peaks of open-door alerts, security incident reports or measuring awareness and knowledge level of employees. If organisation has awareness training in place, they should also measure periodically that personnel have taken the training and passed the course. (Interviewee 1, Interviewee 2, Interviewee 3.) The importance of the communication was emphasized in every aforementioned situation as development among the personnel requires communication to increase awareness of security requirements or organisation's policies (Interviewee 1, Interviewee 2).

### 4.3 Summary

As document analysis concluded, the documents shared a lot of similarities and suggested especially to careful planning and implementation of access control management and visitor procedures as well as to documentation of the policies and procedures. All the documents emphasized the responsibilities of the organisation and individual employee: organisation should develop and manage principles for access control and maintain effective monitoring activities and employees should be instructed to comply with the given guidelines. Application guidelines to electronic access control system by SFS Standardization Finland (2015) was detail specific and provided narrowed information for the thesis scope but at the same time was the only reference in addition to TAPA Facility Security Requirements (2017) and KATAKRI (2015) that clearly suggested to document response procedures for security events.

Throughout the interviews, professionals emphasised the responsibilities of the organisation and employee in a same manner as the documents did. Professionals also stressed the importance of the communication and its relation to security culture creation. Employees can be taught to comply with the given guidelines if they are instructed and reminded to do so periodically. The importance of the documentation for employees but for managers as well was pointed out as the continuity of high-quality management shouldn't be disrupted even if a single responsible employee is absent from the organisation. All professionals agreed that technological solutions support access control monitoring but again emphasised that instructed employees help to create the trouble-free working environment through awareness.

## 5 Products

The results from the data analysis concluded that to comply with the security requirements, Länsi-Uusimaa Department for Rescue Services should have general access control policy underlining the principles and responsibilities for personnel as well as more detailed documents for increasing the security awareness among the personnel such as induction material. The capability to response security events should be upheld in the organisation and therefore detailed response guidelines for relevant security events were created. If personnel are instructed and trained to comply with the given guidelines, the security requirements are met and overall security capability across the organisation will increase.

### 5.1 Access control policy

According to Cambridge Dictionary (2020b), policy is a document underlining "what to do in a particular situation" typically agreed by the management of a business unit or other managing party. Therefore, the access control policy is an important document for case organisation as it sets the basis for general principles and instructs personnel to use facilities securely.

The access control policy already existed in the case organisation, but it was reviewed and updated to give a more comprehensive understanding of security requirements organisation has as well as what are the responsibilities of the personnel concerning physical security. The policy underlines access control management principles, visitor management procedures and basis for key control management and secure access credential use. The principles were mostly based on VAHTI 2/2013 and KATAKRI 2015 requirements. Areal classifications and their protection requirements, access rights and visitor procedures were applied as instructed in VAHTI and KATAKRI by taking into account protected assets and defence-in-depth concept. The following structure of the document was finally developed:

1. Introduction

- the purpose of the policy, security requirements and responsibilities among personnel

2. Physical security, access control and visitor management

- Definition for principles

- Implementation by premises security classification

3. Guidelines for exceptional situations

As specified in the Methodology section, the development of the construction such as guidelines requires evaluation of the product's practicality from the case organisation (Ojasalo et al. 2014, 38). Therefore, the planning officer and head of support from the rescue department was consulted and products were presented for evaluation. The final remarks were done, and the access control policy was ready to be returned. As attachment to policy, short simplified induction material concerning security practices and visitor management process was given to organisation.

## 5.2 Incident response procedures

As reviewed documents concluded, the response procedures should be documented according to KATAKRI, SFS-EN 60839-11-2 and TAPA FSR. Therefore, to monitor access events and possible incident situations more efficiently, the guidelines were created for situation centre operators who are monitoring the access events from the system. By increasing the response capabilities, possible incidents can be solved efficiently, and necessary actions can be taken.

Guidelines were developed by taking into account the nature of the facilities, access control system components and software. The system administrator from rescue department was consulted in this phase to gain more understanding of possible alert situations and how access control system and software works. Response procedures for various alert types were

developed. The guidelines take into account the responsibilities of different stakeholders in alert situations and provides step-by-step guidelines from emerging incident to recovery and reporting phase.

Incident response guidelines were returned to situation unit managers and they agreed guidelines' usability and application to practical work.

# 6 Conclusions and self-assessment

The objective of the thesis was to examine and moreover renew access control guidelines and procedures for the case organisation Länsi-Uusimaa Department for Rescue Services so that the guidelines and procedures would help organisation comply with security requirements. The results from the research process indicated which security requirements should be addressed in the case organisation and how the development of the guidelines would help organisation reach the desired level of security.

The theoretical framework of the thesis presents context of the access control for reader and introduces security requirements from Finnish legislative and rescue perspective. The chosen research methods answered both research questions as document analysis helped to understand security requirement landscape more thoroughly and interviews provided experiences and opinions from security professionals which helped in the development of the guidelines. It can be concluded based on the results that documented responsibilities among the personnel and well-trained procedures help to increase security capabilities in the organisation. The creation of the security culture and awareness itself is still not achieved by addressing requirements in policies but by instructing personnel to understand meaning of the security requirements in everyday work.

The validity of the results is considered to be reliable. The document analysis process is repeatable, and the publicity of the analysed documents is only limited to documents which were retrieved from the case organisation. A shortcoming within the documents is that some of the analysed documents are only available in Finnish and therefore limit the international accessibility of the documents. Professionals who participated to research process through interviews are presented in the thesis anonymously but their expertise and experience in security management is presented to emphasise the validity of the information source. The results from the interviews were similar as professionals' answers were mostly the same and similar to analysed documents as well. Still, it's important to remember that personal opinions might affect the validity of the interview data.

The thesis was done during the winter and spring 2020. The preliminary agreement of the thesis topic with commissioning party was already agreed in December 2019, but the actual research process started in January 2020. In the thesis plan, the timeline for the thesis was

agreed and the deadline for final products' return was set to April 2020. Therefore, the thesis was completed in planned schedule in respect to case organisation's needs.

Even if the final products are left out of the published thesis report, the similar process can be applied in the development of the access control guidelines for other organisations or companies. The document analysis presents how careful planning and implementation of e.g. access rights and responsibilities should be applied. Analysed information from the documents is supported by the results from interviews and results share lot of similarities.

As thesis writer and employee, I have gained more understanding of the importance of the access control and management as part of the overall physical security. The thesis process was educational as it taught me to view security management from more comprehensive view and to combine research approach to development. During the thesis process, I have been applying project management principles, communicating with various professionals and learned to present my ideas and ask for consultation if needed.

References

Printed sources

Fennelly, J. 2013. Effective Physical Security. 4th edition. The United Kingdom: Elsevier.

Flick, U. 2011. Introducing Research Methodology: A beginner's guide to doing a research project. London: Sage.

Hirsjärvi, S. & Hurme, H. 2000. Tutkimushaastattelu: teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2014. Kehittämistyön menetelmät: Uudenlaista osaamista liiketoimintaan. 3. uudistettu painos. Helsinki: Sanoma Pro.

Electronic sources

Cambridge Dictionary. 2020a. Meaning of requirement in English. Accessed 11.2.2020. https://dictionary.cambridge.org/dictionary/english/requirement

Cabridge Dictionary. 2020b. Meaning of policy in English. Accessed 30.3.2020. https://dictionary.cambridge.org/dictionary/english/policy

Deloitte. 2019. Miten uusi tiedonhallintalaki vaikuttaa viranomaisiin? Toiminnan digitalisointi, tietoturvallisuus ja tiedon jakaminen korostuvat uudessa tiedonhallintalaissa. Accessed 14.1.2020. https://www2.deloitte.com/content/dam/Deloitte/fi/Documents/risk/Miten%20uusi%20tiedonhallintalaki%20vaikuttaa%20viranomaisiin.pdf

EU. 2016. General Data Protection Regulation 2016/679. The European Union. Accessed 14.1.2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC

Finance Finland. 2017. Avainturvallisuusohje. Turvallisuusohje. Finanssiala. Accessed 14.1.2020. https://www.finanssiala.fi/vahingontorjunta/dokumentit/Avainturvallisuusohje.pdf

Finland 1999. Act on the Openness of Government Activities 621/1999. Accessed 14.1.2020. https://www.finlex.fi/en/laki/kaannokset/1999/en19990621_20150907.pdf

Finland 2010. Government Decree on information security in central government 681/2010. Accessed 14.1.2020. https://www.finlex.fi/en/laki/kaannokset/2010/en20100681.pdf

Finland 2011. Rescue Act 2011/379. Accessed 20.11.2019. https://www.finlex.fi/en/laki/kaannokset/2011/en20110379.pdf

Finland 2015. Act on Operation of the Government Security Network 10/2015. Translated from Laki julkisen hallinnon turvallisuusverkkotoiminnasta. Accessed 8.12.2019. http://finlex.fi/fi/laki/alkup/2015L/20150010

Finland 2019. Act on Information Management in Public Administration 906/2019. Translated from Laki julkisen hallinnon tiedonhallinnasta. Accessed 14.1.2020. https://www.finlex.fi/fi/laki/alkup/2019/20190906#Lidp446978592

Kovacich, G. & Halibozek, E. 2003. The Manager's Handbook for Corporate Security: establishing and managing a successful assets protection program. Butterworth-Heinemann. Book from Ebook Central. Accessed 10.1.2020.

Lorenzi, N. 2018. Access control devices offer security solutions. Health Facilities Management Vol. 31 Issue 2. Article from ProQuest database. Accessed 13.1.2020.

Länsi-Uusimaa Department for Rescue Services. 2017. Rescue Department. Accessed 20.11.2019. https://www.lup.fi/en-US/Rescue_Department

Ministry of Defence. 2015. Katakri. Information security audit tool for authorities. Accessed 14.1.2020. https://www.defmin.fi/en/administrative_branch/defence_security/katakri_2015_-_information_security_audit_tool_for_authorities

Ministry of the Interior. 2019. Rescue departments. Ministry of the Interior. Department for Rescue Services. Accessed 20.11.2019. http://www.pelastustoimi.fi/rescue-services/rescue-departments

Norman, T. 2012. Electronic access control. Butterworth-Heinemann. Book from Ebook Central. Accessed 13.1.2020. https://ebookcentral.proquest.com/lib/laurea/reader.action?docID=787245

Open Security Architecture. N.d. IT Security Requirements. Accessed 11.2.2020. https://www.opensecurityarchitecture.org/cms/definitions/it_security_requirements

Oyegoke, A. 2011. The constructive research approach in project management research. Journal of Managing Projects in Business 4(4). Accessed 15.1.2020. https://www.researchgate.net/publication/241558478_The_constructive_research_approach_in_project_management_research

Saunders, M. 2015. Research Methods for Business Students. England: Pearson Education. Book from Ebook Central. Accessed 8.12.2019.

SFS Standardization Finland. 2017. ISO/IEC 27002:2017 Information technology. Security techniques. Code of practice for information security. Accessed from SFS online portal 14.1.2020.

SFS Standardization Finland. 2015. SFS-EN 60839-11 Alarm and electronic security systems. Part 11-1 and 11-2. Finnish Standards Association. Accessed from SFS online portal 14.1.2020.

TAPA. 2017. Facility Security Requirements. Transportation Asset Protection Association. Accessed 14.1.2020. https://www.tapa-apac.org/wp-content/uploads/2019/11/TAPA_FSR_2017_Final-March-2017.pdf

Terschuren, P. 2016. Visitor Management Options Enhance Front Door Security. Security Magazine. Accessed 13.1.2020. https://www.securitymagazine.com/articles/87240-visitor-management-options-enhance-front-door-security

Valtiovarainministeriö. 2013. Toimitilojen turvallisuusohje. Translated to Office Premises Information Security Instructions. Accessed 14.1.2020. https://www.vahtiohje.fi/c/document_library/get_file?uuid=78751ee8-c2c8-4ac4-945c-72cb9ec4a01b&groupId=10229

Valtiovarainministeriö. 2015. Turvallisuusverkko varmistaa johtamista ja viranomaisviestintää kaikissa oloissa. Accessed 11.2.2020. https://valtioneuvosto.fi/artikkeli/-/asset_publisher/10623/turvallisuusverkko-varmistaa-johtamista-ja-viranomaisviestintaa-kaikissa-oloissa

Unpublished sources

Interviewees. Interviews with the author. January & February 2020. Personal communication.

Länsi-Uusimaa Department for Rescue Services. 2013. Liikkuminen ja toimitilasuojaus pelastuslaitoksen toimitiloissa. Accessed 14.1.2020.

Pelastuslaistosten kumppanuusverkosto. 2019. Pelastustoimen tietoturvallisuus. Principle manual. Accessed 14.1.2020.

Pelastuslaistosten kumppanuusverkosto. 2019. Pelastustoimen tilaturvallisuusohje. Principle manual. Accessed 14.1.2020.

Figures and tables

Figures



Tables

Appendices

Appendix 1: Materials analysed in document analysis

| Document | Author | Year | Main audience | Purpose |
|---|---|---|---|---|
| Internal policies and guidelines | | | | |
| Liikkuminen ja toimitilasuojaus pelastuslaitoksen toimitiloissa (current access control policy) | LUP | 2013 | Personnel of the organisation | Provide common guidelines for case organisation personnel |
| Pelastuslaitosten tietoturvallisuus (Information security guidelines for rescue departments) | Pelastuslaitosten kumppanuusverkosto | 2019 | Rescue departments in Finland | General guidelines for rescue departments in Finland |
| Pelastuslaitosten toimitilaturvallisuus (Physical security guidelines for rescue departments) | Pelastuslaitosten kumppanuusverkosto | 2019 | Rescue departments in Finland | General guidelines for rescue departments in Finland |
| External policies, requirements and guidelines | | | | |
| Government Decree on Information Security in Central Government 681/2010 | Finland | 2010 | Central government, government agencies | Regulation on information security requirements |
| Laki julkisen hallinnon tiedonhallinnasta (Act on Information Management for Public Authorities) 906/2019 | Finland | 2019 | Governmental agencies, public authorities | Regulation on information management, including information security requirements |
| The General Data Protection Regulation | European Union | 2016 | Companies, organisations | Improve the protection of personal data |
| KATAKRI: Information Security Audit Tool for Authorities | Ministry of Defence | 2015 | Companies, organisations | Audit tool |
| VAHTI 2/2013: Toimitilojen tietoturvaohje (Office premises information security instructions) | Ministry of Finance | 2013 | Central government, governmental agencies | Guidelines on physical security planning and implementation as part of the information security |
| SFS-EN 60839-11-2 Electronic access control system. Application guidelines | SFS Standardization | 2015 | System owners | Guidance and requirement for installation and operation of EACS |
| Avainturvallisuusohje (secure key control guidelines) | Finance Finland | 2017 | Companies and organisations | Prevent damage and limit the amount of damage |
| ISO/IEC 27002:2017 | SFS Standardization | 2017 | Companies and organisations | Reference for control selecting as part of ISMS |
| Facility Security Requirements | TAPA: Transported Assets Protection Association | 2017 | Companies and organisations | Standard for securing storages and facilities |

Table 2: Summary of materials

Appendix 2: Interview questions

Background of the participant: position, experience in years, working environment, relation to physical security and access control management

**Theme 1: Responsibilities**

- Who is in charge of managing access control guidelines and procedures?
- Who is monitoring access control in the organisation?

**Theme 2: Identification and monitoring of security incidents**

- Are personnel of the organisation trained to react on security events?
  What kind of events? How to react?

**Theme 3: Maintenance and other contractors in the facilities**

- How access and key control of third-party operators (e.g. cleaning, maintenance) has been managed in the organisation?

**Theme 4: Visitor management**

- How personnel of the organisation have been trained to visitor management?
- What kind of pains and gains are related to visitor management processes?

**Theme 5: Developing the procedures**

- Pains and gains faced in access control guidelines and procedures in the organisation?
- Communication of facility security and security requirements among the organisation's personnel: how, when?